Multi-State Lottery Association

Random Number Generator Report
Executive Summary
March 01, 2018

Game Drawing Services Agreement:

On May 18, 2014, the Multi-State Lottery Association (MUSL) entered into a Game Drawing Services Agreement (Agreement) with the Arizona Lottery (Arizona). The Agreement was subsequently amended on September 15, 2015. The purpose of the Agreement was to have MUSL perform electronic random number generator (RNG) drawings for Arizona state games.

In June-July 2015, MUSL built three (3) RNGs for this purpose. AZ RNG2 and AZ RNG1 were used and secured in MUSL's draw room. AZ RNG3 was sent to Arizona as a potential backup machine and/or to perform other state drawings or raffles. On April 15 and again on July 2, 2015, BMM Testlabs provided Compliance Certifications for *MUSL Quantum Vision v2.0.0.0 using the Micro Roentgen Radiation Monitors* (Model RM-60). Quantum Vision v2.0.0.0 was installed and was operated on all three machines.

Incidents:

On Wednesday, October 4, 2017, Arizona officials notified MUSL's Executive Director that the same game numbers were repeating on consecutive draws. Four Arizona games (Pick 3, Fantasy 5, All or Nothing and 5 Card Cash) were affected between September 21 and October 03, 2017. Arizona and MUSL Staff isolated the issue to one machine, AZ RNG2, and immediately removed and secured it for testing.

On October 9, November 15 and November 21, 2017, the same Arizona Pick 3 numbers (8-0-4) were selected from the remaining RNG, AZ RNG1. No other Arizona games were affected. MUSL's internal auditor examined the pre-post and post-draw tests and found the results to be within expected norms. On November 22, 2017, out of an abundance of caution, AZ RNG1 was also removed from service and secured, pending third party testing.

Actions:

The Arizona Lottery Executive Director notified MUSL's Executive Director of the above events. In accordance with MUSL's IT Incident Response Plan, MUSL's Executive Director notified the Board President and Audit Committee Chair and instructed the Chief Audit Executive to immediately initiate an independent review of the events. All actions and findings were under the auspices of the Audit Committee.

An independent third-party forensic technology firm tested the hardware in both AZ RNG2 and AZ RNG1 and the RM-60 monitor from AZ RNG3. The firm also performed a limited review of the source code.

An independent statistical expert was also hired to evaluate the probability and frequency of Pick 3 numbers repeating and compare expected results to the actual AZ RNG1 draw events.

Test Results:

AZ RNG2 (numbers repeating on consecutive draws)

- Hardware Failure
  MUSL's digital draw systems contain an analog Geiger counter (RM-60). The RM-60 measures the radioactive output from a commercially available synthetic element called Americium. The measurement results in a 32-bit true random number, which is used to seed the algorithm that generates the draw results. The RM-60 was tested and deemed inoperative.

  The manufacturer indicated that in certain circumstances the RM-60 radiation monitor may overheat resulting in the fracture of an internal glass tube. The impact of which renders the RM-60 inoperative.
- Source Code
  MUSL's software retrieves a 32-bit random number generated by the aforementioned RM-60. These numbers become the algorithmic seed that generates game results. The RM-60 software attempts to generate a 32-bit random number five times, and MUSL's code attempts to retrieve it five times. After five attempts, the generation and retrieval process stops. If the retrieval process is unsuccessful, MUSL's software does not stop but continues until the program has executed. As a 32-bit random number was never generated or retrieved, the underlying algorithm executes using a default setting of zero. The exact same seed, zero in this case, will always create the same winning numbers, and assuming no other factors influence the algorithmic selection.

Conclusion AZ RNG2:
The forensic firm concluded that the RM-60 in AZ RNG2 was inoperative. The faulty hardware was therefore unable to generate a random number seed. This ultimately resulted in MUSL's game algorithm using a seed of all zeros. Additionally, MUSL's code did not contain a function to stop the draw if the RM-60 failed. The same seed will always produce the same results, thus identical numbers on consecutive draws.

AZ RNG1 (Pick 3):
AZ RNG1 was removed from service after 8-0-4 appeared in drawings on October 9, November 15 and November 21, 2017. AZ RNG1 was tested by the aforementioned independent third-party forensic technology firm. Additionally, draw results for Pick 3 were evaluated by an independent statistical expert and are described below.

Conclusion AZ RNG1:
The RM-60 in AZ RNG1 was tested and deemed to be operating within the manufacturer's guidelines and generating apparently valid results. (See Statistical Analysis below.)

AZ RNG3:

AZ RNG3 (the back-up machine) is not in scope for this review with the following caveat. After AZ RNG2 was removed from service, Arizona attempted to activate AZ RNG3 as part of a draw contingency plan. Arizona draw staff concluded that AZ RNG3 was inoperative and contacted MUSL. MUSL personnel flew to Phoenix, examined the machine and replaced the internal analog Geiger counter. After replacing the RM-60, Arizona and MUSL personnel concluded that AZ RNG3 was now operational.

Conclusion AZ RNG3:

The old RM-60, removed from AZ RNG3, was subsequently tested by the aforementioned independent third-party forensic technology firm and deemed inoperative.

Statistical Analysis (AZ RNG1 - Pick3)

Background:

As a precautionary measure, noted above, MUSL AZ RNG1 was also removed from service in response to the following events:

1. AZ RNG2 hardware failure and repeating game results, and
2. Potential patterns in Pick 3 game results.

Objective and Scope:

An independent statistical expert was engaged to evaluate the probability and frequency that three numbers, each ranging from zero to nine, would repeat within a draw population of 742 events. The purpose of this exercise was to determine whether actual Pick 3 results were consistent with predicted outcomes.

Conclusion:

Based upon the evidence of three comparative examinations, it does appear that what transpired, in aggregate across the 29-month period, is largely consistent with what one would expect to see probabilistically. Although there were a few instances when the same 3-digit numbers appeared, the models would indicate that this is to be expected. Similar conclusions can be stated when examining each of the three digits separately, or any of the three pairs of digits separately. There were some small deviations from expected outcomes (i.e., anomalies) contained within the data, but these will typically be present in such data, even if the draw mechanisms are working appropriately.

Furthermore, and this is the key, if we go back to our full set of 742 observations, it is not unreasonable to have a small set of three-digit numbers occur 3, 4, or even 5 times among the set of winners. In our data, no (set of) number(s) occurred more than 5 times, with only two numbers occurring exactly 5 times (8-0-4 and 9-1-9). Thus, it is within the realm of what might occur naturally for 8-0-4 to have occurred 5 times between 7/15 and 11/17.